ABSTRAK

Di era teknologi informasi dan komunikasi sekarang ini, pertukaran informasi dilakukan melalui internet. Informasi yang dikirim pun seringkali berupa informasi yang rahasia, berupa gambar, suara atau video. Sehingga diperlukan suatu algoritma keamanan yang memberikan jaminan keamanan informasi dan juga waktu proses algoritma yang cepat, agar tidak mengganggu proses pengiriman informasi. Pada tugas akhir ini, telah dirancang algoritma keamanan, yang digunakan untuk melakukan proses enkripsi-dekripsi gambar.

Pada tugas akhir ini menggunakan dua algoritma yaitu algoritma AES *(Advanced Encryption Standart)* dan algoritma *Chaos*. Algoritma *Chaos* yang digunakan adalah Arnold's Cat Map yang digunakan untuk melakukan proses pixel shuffling dan Henon Map yang digunakan untuk proses encoding. Kedua algoritma akan dibandingkan, sehingga akan diperoleh algoritma enkripsi gambar yang lebih baik.

Hasil yang diperoleh dari pengujian yang dilakukan pada tugas akhir ini algoritma *Chaos* memiliki performansi yang cukup untuk diimplementasikan pada enkripsi gambar. Algoritma *Chaos* memiliki waktu komputasi yang lebih cepat daripada algoritma AES. Dari *cipherimage,* kedua algoritma sama-sama menghasilkan *cipherimage* dengan histogram yang *uniform*. Nilai koefisien korelasi *cipherimage* kedua algoritma pun sma-sama mendektai 0. Ketika kedua algoritma diuji dengan noise AWGN, algoritma *Chaos* mampu bertahan lebih baik daripada algoritma AES. Hal ini ditunjukkan dengan nilai PSNR algoritma *Chaos* memiliki nilai lebih besar dibanding algoritma AES. Algoritma *Chaos* memiliki nilai BER lebih kecil daripada algoritma AES. Sedangkan nilai avalanche effect algoritma AES mendekati 50% yang berarti lebih unggul dibanding algoritma *Chaos* yang hanya 15%. Untuk durasi waktu brute force attack, algoritma AES memiliki waktu $1.68\ x\ 10^{20}$ tahun sedangkan algoritma *Chaos* $2.206\ x\ 10^{12}$ tahun

Kata kunci : *Chaos, Arnold's Cat Map*, *Henon Map* , enkripsi, AES